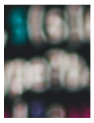
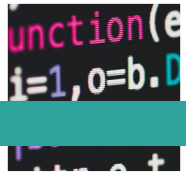
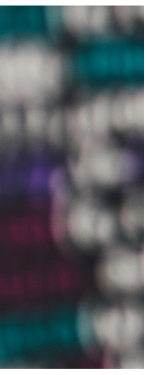
The Future of Data Privacy & Marketing

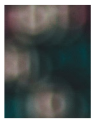
Authors and Contributors:

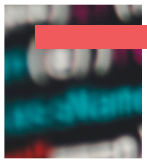
Sarah Stein
Amy Ard
Kacie Meixel
Steve Parker Jr.











A Levelwing Whitepaper

What is the future of marketing in an era of increased consumer data privacy awareness and regulation? **Read the Levelwing whitepaper for insight.**

Table of Contents

The Rules Are Changing:

What The Future of Data Privacy Will Mean For Marketing

Summary

As the complexities of data privacy regulations grow, businesses are re-evaluating their marketing programs and taking a proactive approach to stay abreast of developing changes. One of the most prominent challenges they now face is striking a balance between preserving user privacy while maintaining a personalized customer experience. With a deep understanding of regulations integrated with an effective digital strategy to retain customers, brands can successfully use emerging data privacy laws to their advantage.

Finding Common Ground

> *"To participate in modern life is to scatter millions of digital traces, data points, and personal information in our wake."*[1]

In this quote, author Sarah Brayne illustrates the reality of the digital age we're living in. Today, consumers are continually offering up privacy-sensitive data – not unconsciously – yet, in a way that the implications of such sharing may not be fully understood. Users submit some personal information willingly, while some is gathered automatically through technology such as cookies. Either way, the digital footprint left behind as we constantly use the technology at our disposal is a prized commodity for most businesses.

As the public's heightened awareness of consumer data commoditization grows, so do the fears associated with the control and regulation of this data. A recent survey by Pew Research Center revealed that the majority of Americans are concerned with the collection and use of their data by both companies and the government. The survey reports that most U.S. adults say their personal information is less secure now than it was five years ago, with over 80% of Americans feeling that they lack control over what personal data is collected about them.[2]

So, how can consumers and companies find common ground between data privacy and customer experience? What measures should be taken by businesses to ensure compliance while at the same time, develop innovative ways to maintain customer relationships?

sources

1. Brayne, S. (2021). Predict and surveil: Data, discretion, and the future of policing. New York, NY: Oxford University Press.
2. https://internetinnovation.org/op-eds/congress-is-finally-listening-to-consumers-on-internet-privacy/

What businesses need now is a plan.

In this whitepaper, we'll review General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), the privacy laws that have made the most impact on future privacy protections, including the most recent expansion and amendment to CCPA – California Privacy Rights Act (CRPA). We'll also highlight the ways businesses and marketers can leverage what we've learned thus far to future-proof data privacy principles and strike a balance between remaining compliant with regulations and finding new ways to target and retain customers. Since consumer data progressively drives the growth of innovation and marketing, it should be no surprise that privacy regulation will affect the evolution of how businesses sell their products and services. Here's a review of the laws that have changed the landscape of data privacy and ushered in a new era of regulations.

Data Privacy Regulations: The Journey To Now

If we want to predict and prepare for what's to come, we need to start from the beginning. In May 2018, any organization worldwide that offered goods and services to residents of the European Union (and controlled or processed personal data relating to those individuals) was required to comply with GDPR whether or not the organization itself was located within the E.U.

A Review of GDPR:
The Main Points

CONSENT

Companies need explicit consent before collecting, storing, or giving out user data

OBJECTIONS

Data subjects can object to how their data is used

DOCUMENTATION

Companies must keep detailed documentation of their stored data

ACCESS TO INFORMATION

Users can request documentation of their data being held

DATA ERASURE

Users have the right to request the removal of their personal information

DATA CHANGES

Users can request that inaccurate stored information can be corrected

What are the consequences of non-compliance?

Depending on the rule breached, organizations can be charged up to €20,000,000 or up to 4% of the total worldwide annual revenue of the preceding financial year.[3]

Two years in, we've seen both opposition and acclaim for GDPR from citizens, politicians, and businesses. On one hand, 62% of UK consumers feel more comfortable sharing their data and are more aware of their rights. On the other hand, many businesses feel the pressure financially as they add resources to support compliance, such as legal counsel and data protection officers. Regardless, GDPR has paved the way for new changes and an expansion in data regulation that has reached far beyond the E.U.

sources

3. https://gdpr.eu/fines/

GDPR:
Setting Privacy Regulations In Motion Worldwide

This new set of regulations began a worldwide eye-opening of sorts, as a wave of data privacy laws began to wash over governments internationally. Over 80 countries and independent territories, including nearly every country in Europe and many in Latin America, the Caribbean, Asia, and Africa, have now adopted comprehensive data protection laws.[5]

Individual U.S. states have begun creating their own patchwork of sector-specific laws that apply to industries such as telecommunications, healthcare, data brokers, financial institutions, and more. Bills or bill drafts have been introduced/filed in at least 25 states and Puerto Rico.[6] While they won't be the same as other broader consumer data privacy laws, they will encompass similar state-specific requirements. As the COVID-19 pandemic brought a significant shift in individuals' and businesses' priorities, many legislative actions, including data privacy, have been put on the political backburner. However, attention to the topic is likely to resurface in 2021 as privacy legislation gains more traction regarding COVID-related information such as tracking and tracing cases, which require data collection and processing activities that involve privacy risks. [7]

While there is not one singular federal law that governs data security and privacy in the U.S., as of 2019, there were at least 13 federal-level data privacy bills pending in Congress.[8] Over time support for a comprehensive federal mandate has grown, however, due to the complicated nature of having to comply with each state's unique privacy regulations it is doubtful we will see federal privacy legislation enacted within the next year. Nonetheless, it is extremely important for businesses to remain compliant and vigilant. Data-driven marketing and privacy innovation will prove imperative to enhance competitive advantage as data continues to be a valuable business asset.

sources

4. https://www.varonis.com/blog/gdpr-effect-review/
5. Greenleaf, Graham, Global Data Privacy Laws: 89 Countries, and Accelerating (February 6, 2012). Privacy Laws & Business International Report, Issue 115, Special Supplement, February 2012, Queen Mary School of Law Legal Studies Research Paper No. 98/2012, Available at SSRN: https://ssrn.com/abstract=2000034
6. https://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx
7. https://www.natlawreview.com/article/election-2020-looking-forward-to-what-biden-presidency-may-mean-data-privacy-and
8. https://rampedup.us/marketing-data-privacy-regulations/

CCPA:

Often referred to informally as the “American version of GDPR,” California passed the most comprehensive state data privacy legislation to date as of January 1, 2020. Known officially as the California Consumer Privacy Act (CCPA), this legislation was created to require a range of controls to protect privacy, ensure security, and allow the residents of California to retain ownership of their data and how it is used. With many of the world’s major tech organizations stationed in California, the potential for global repercussions of these regulations were pushed into the spotlight.

A Review of CCPA:
The Main Points

Like GDPR, CCPA protects any information that can be used to directly or indirectly identify the person or “data subject,” which includes, but is not limited to:

- NAME
- PHONE NUMBER
- EMAIL ADDRESS
- SOCIAL MEDIA POSTS
- IP ADDRESS AND COOKIES
- VIN NUMBER
- UNIQUE PERSONAL IDENTIFIER

What are the consequences of non-compliance?
Depending on the rule breached, organizations can be charged up to $7,500 for each internal violation and $2,500 for each unintentional violation. Enforcement of these consequences began on July 1, 2020.

Ammendments and Expansions of CCPA: CPRA and What It Means For The Future

Approved by 56% of California voters[9], the California Privacy Rights Act of 2020 – an initiative to expand and amend CCPA – passed on the ballot in November 2020. Moving California's data protection laws closer to GDPR standards, CPRA began the development of the California Privacy Protection Agency to enforce the regulations, and closed some of the potential loopholes CCPA allowed, such as the ability of businesses to resolve violations before being penalized for said violations. The initiative enforces more stringent provisions, with the majority taking effect beginning January 1, 2023.

Key Takeaways From CPRA

DEFINITIONS AND AMENDMENTS

"Sensitive personal information" is a new legal definition created by the CPRA. Race/ethnic origin, health information, religious beliefs, sexual orientation, Social Security number, biometric/genetic information, and personal message contents all fall under this definition.

In addition to revising specific definitions within the act, it will also require businesses to do the following:

- LIMIT A CONSUMER'S PERSONAL INFORMATION UPON THE CONSUMER'S REQUEST;
- PROVIDE CONSUMERS WITH AN OPT-OUT OPTION TO RESTRICT THEIR SENSITIVE PERSONAL INFORMATION, AS DEFINED IN LAW, FROM BEING USED OR DISCLOSED FOR ADVERTISING OR MARKETING;
- OBTAIN PERMISSION BEFORE COLLECTING DATA FROM CONSUMERS WHO ARE YOUNGER THAN 16; OBTAIN PERMISSION FROM A PARENT OR GUARDIAN BEFORE COLLECTING DATA FROM CONSUMERS WHO ARE YOUNGER THAN 13;
- CORRECT A CONSUMER'S INACCURATE PERSONAL INFORMATION UPON THE CONSUMER'S REQUEST.[10]

sources

9. https://www.prnewswire.com/news-releases/california-voters-decisively-approve-prop-24-the-california-privacy-rights-act-301166408.html
10. https://ballotpedia.org/California_Proposition_24,_Consumer_Personal_Information_Law_and_Agency_Initiative_(2020)#cite_note-text-1

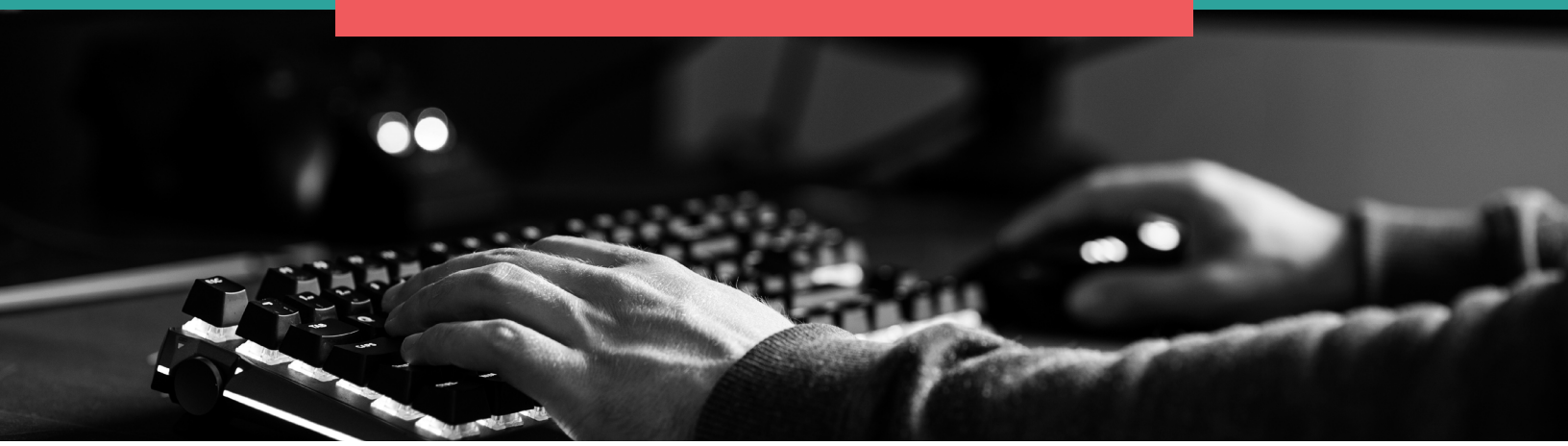
Key Takeaways From CPRA
cont.

WHY IT MATTERS

In the E.U. and U.S., people generally have the right to know when data is being collected. The notice of this collection can come in many ways, but should be in writing, clear, understandable, and conspicuous. In the EU, generally data may only be used as described in notice if a person opts-in. In the US, generally data may only be used as described in notice if a person opts-out.

In a recent update on privacy law trends by Hutnik & Burstein (2020), an amendment to CCPA is explained: the distinction between "sharing" as opposed to "selling." Within the distinction, personal information has been defined as "disclosing or otherwise communicating a consumer's personal information for 'cross-context behavioral advertising' (defined as ad targeting based on information obtained about a consumer across different apps or services) whether or not for monetary or other valuable consideration, including transactions between a business and a third party." Though CPRA will remain opt-out-based, the expanded definition of "sharing" may have a greater impact on digital marketing contracts and will widen the opt-out obligations of businesses even further.[11]

The update goes on to offer an example: If a business makes the decision that their disclosures of a user's personal information does not fall under "sales" since the exchanges do not involve valuable consideration, those businesses may need to re-think that decision. Any business that engages in "selling" or "sharing" must also provide consumers with an opt-out link that gives them a "Do not sell or share my personal information" option. (Hutnik & Burstein, 2020)



sources

11. https://www.adlawaccess.com/2020/11/articles/its-here-california-voters-approve-the-cpra/

The Costs Of Non-Compliance

Data privacy can no longer be ignored by companies large or small. While many have already conformed to the new regulations, some have faced the consequences of non-compliance — intentionally or not.

As of one year ago, 52.8% of U.S. digital marketers feel the threat of regulation as a challenge that might impede their ability to derive value from their data-driven marketing initiatives.[12]

Both agencies and in-house marketing departments alike need to be aware of how they use, collect, and store data. While marketers and their agencies won't necessarily be held liable under regulations such as CPRA, they will need to do more due diligence regarding the data they use to reach consumers.[13] Because third parties are sometimes used to enhance data for audience building and targeting, marketers will need to be extra diligent to find out the source of that data.

sources

12. https://www.varonis.com/blog/gdpr-effect-review/
13. https://www.ama.org/2019/05/30/the-impact-of-gdpr-and-ccpa-on-digital-marketers/

Beyond the challenges of deleting personal information—due to fragmented infrastructure or third-party networks—the most common concerns include:

RISK OF LITIGATION OR FINES

As of May 25, 2019, GDPR's first anniversary, enforcement actions resulted in €56,000,000 in fines, and as of January 2020, total fines have risen to €114,000,000. Hundreds of cases are still under review with European data privacy authorities.[14] Some companies have taken to blocking traffic from Europe entirely to avoid any risk of penalties.

Smaller businesses are not immune. Businesses lacking the same resources to adapt their policies and practices quickly are the ones who will suffer most. Considering the rising expense of data management technology tools and legal consulting, the cost for businesses to comply has been estimated at $100,000.[15] Annually, a larger chunk of budgets will need to be set aside for legal counsel and data security efforts – including in-house or outsourced data protection officers.

LOSS OF REVENUE

Plain and simple, businesses that appear to threaten a consumer's privacy are going to lose revenue. Brands will suffer reputation damage if they fail to correct shadowy data practices or comply with regulations. Even in areas that regulations don't cover, consumers demand ethical behavior – especially with sensitive data. Privacy practices that make it difficult to opt out, use complex or confusing language, or push users to consent to broad data sharing will be denounced, which in response may cause consumers to remove their data from a firm's database or provide false information.

Without the trust of consumers – and the accompanying information they willingly provide – marketing tactics such as lookalike audience targeting or remarketing, budgets spent on media become a lost cause. The long-term loss of revenue suffered by driving away customers with dubious privacy practices or the use of overreaching personal data is greater than any fine imposed.

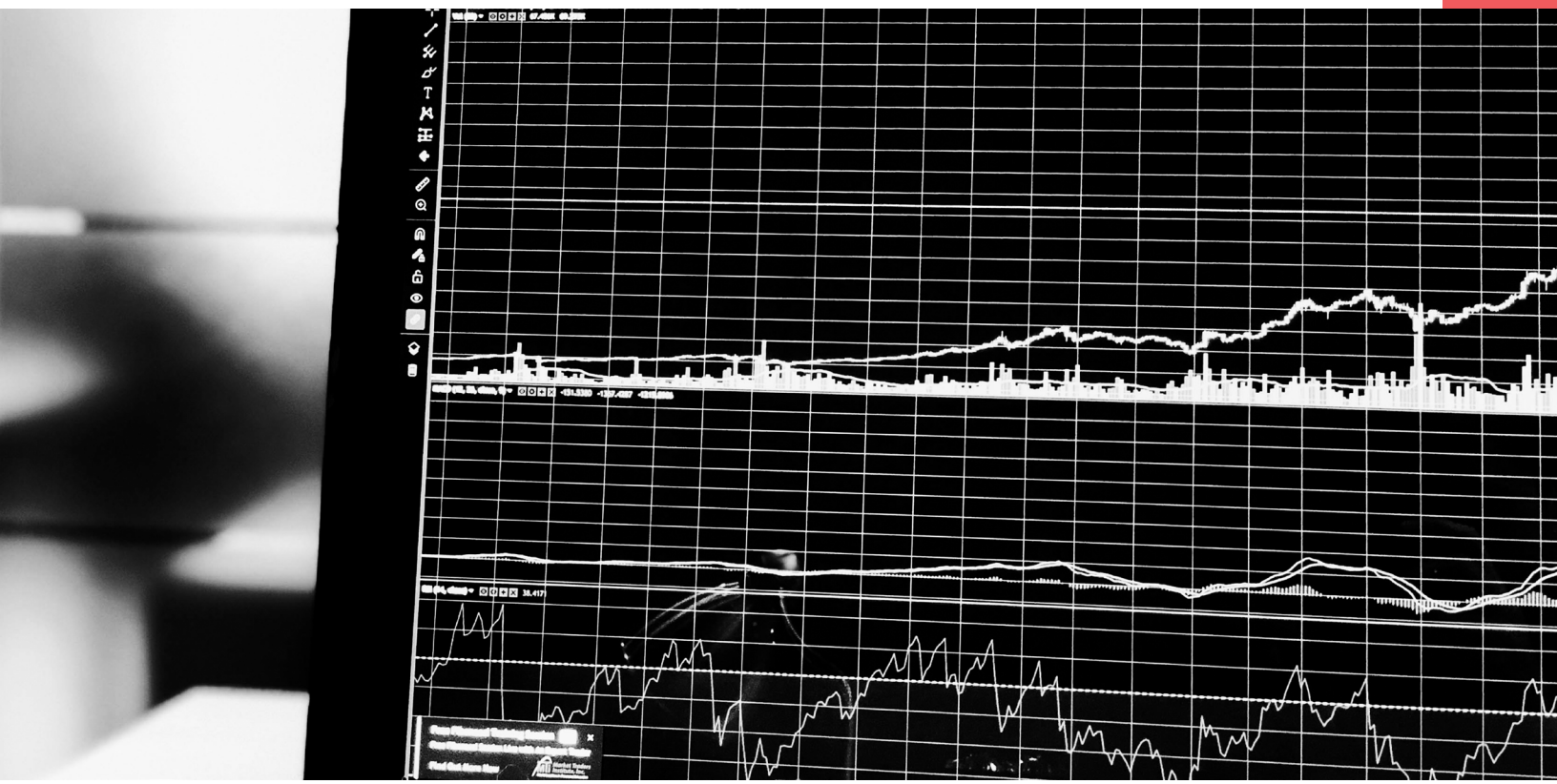
sources

14. Frazier, J. (2020). Corporate Data Privacy Today:A Look at the Current State of Readiness, Perception and Compliance.www.static2.ftitechnology.com
15. https://www.securityinfowatch.com/cybersecurity/information-security/article/21079552/the-impact-of-data-privacy-regulations-greater-on-small-businesses

LOSS OF CUSTOMER LOYALTY AND TRUST

High profile consumer data breaches, along with popular documentaries like 'The Great Hack' and 'The Social Dilemma,' have had a direct impact on how consumers feel about sharing their personal information. "The scale of consumer data exposed in the most catastrophic breaches is staggering." (Anant et al., 2020) In two breaches at one large corporation, more than 3.5 billion records were made public.[16] The result of these scandals and other distressing news stories: 57% of consumers don't trust brands to use their data responsibly.[17]

Take a home automation assistant, for example. Many consumers fear that a product that seems to be "always listening," is the perfect opportunity for a company to sell their usage habits to advertisers. These types of privacy concerns cause customers to be less motivated to share personal information that could perpetuate a relationship with the company, cutting off chances of future purchases or long-term customer loyalty. In the U.S., 87% of consumers say they will take their business elsewhere if they don't trust that the company is handling their data responsibly.[18]



sources

16. https://www.mckinsey.com/business-functions/risk/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative
17. https://www.cim.co.uk/newsroom/opinion-be-transparent-on-social-media-or-risk-the-consequences/
18. https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/cybersecurity-protect-me.html

The potential for a cookie-less future

Put simply, the purpose of the cookie is to help a website keep track of visits and activity. For instance, it helps many online retailers make the shopping experience easier by keeping track of what items are in a customer's cart. Cookies track user data that is analyzed and used to develop algorithms that can make systematic recommendations and predictions to personalize the customer experience. Cookies fuel the digital advertising world, but with recent tightening of privacy regulations, many marketers are looking at the possibility of the removal of 3rd party cookies completely.

In anticipation of a cookie-less future, marketers can implement these three changes to continue to deliver personalized experiences across a multitude of consumer touchpoints:

Allow consumers to be forgotten with an opt-out cookie policy on websites.

Integrate and leverage 1st party and 2nd party data using Customer Data Platforms (CDP) to reach prospects and customers in a more targeted way using their own channels along with paid media.

Implement media plans testing with results generation using the new data.

Within the digital marketing environment, a cookie-less, permission rich future presents both challenges and opportunities. To spot opportunities for innovation, those looking for guidance will need to maintain vigilance to the constant changes that are taking place and understand the disruption that is likely in the near future.

What Consumers Want

In a survey conducted by McKinsey, 1,000 North American consumers revealed that they are becoming increasingly intentional about what types of data they share – and with whom.[19] Not only is sharing personal data a matter of trust, it is also a matter of personal gain.

Recognizing the value of their personal data, here's a hierarchy of what consumers want in return for its use:

39% of respondents like the idea of monetary compensation from a company for sharing their personal data

20% most value promotion incentives and discounts based on their interests

16% value convenience and speed in using their service

14% more responsive customer service and support

11% would exchange their data for creation of new services and products[20]

Getting a new perspective

At the start of GDPR, marketers and businesses uniformly felt the anxiety that came with notions of tracking limitations, or incomplete reports, wondering if they would be "running blindly" without a complete or accurate view of ROI.

Contrary to popular perception, these new data privacy laws and regulations have shown to have unlikely benefits. But how?

Two opportunities have emerged from the changes to data protection and privacy.

Enterprises can:

IMPROVE THEIR CONSUMER CONFIDENCE

BOLSTER THEIR COMMITMENT TO KEEPING CONSUMER DATA SAFE

sources

19. https://www.mckinsey.com/business-functions/risk/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative
20. https://www.prnewswire.com/news-releases/survey-shows-consumers-very-willing-to-trade-personal-data-for-financial-benefits-301106196.html

Opportunities to improve confidence and trust

Brands should be buoyed by the fact that 47% of consumers say they trust companies which let them control how their personal data is used. More encouraging still is the fact that 37% say they tend to spend more money with these brands as a result.[21]

"Customers value judicious use of data within a relationship of trust. That trust is based on having the appropriate security, privacy and ethical controls in place to protect personal information," said Gilbert Hill, CIPM, CEO of TapMyData, a developer of customer rights and identity management software and a member of the Data Marketing Institute U.K.'s Responsible Marketing Committee. "When we treat consumers with respect and outline the benefits to them of capturing their data, we'll be pleasantly surprised with their reaction. Smart brands are able to do that in clever, nuanced ways that bring customers closer."[22]

As consumers gain more visibility into who, what, and how their information is being used, insight can be gleaned through consent as to what individuals' interests are, and therefore provide them with information that they want to receive. Despite the decrease in scale of available data, what is leftover is much higher quality, cleaner, more reliable data sets. This helps to remain compliant, while at the same time, helps to segment customers more accurately and focus communication based on specific interests.

The key takeaway:

Culling data sets down to the most productive and valuable customer contacts – and marketing more creatively to them – will improve the cost vs. benefit ratio of retaining this data while also lowering liability.

sources

21. https://www.marketingweek.com/consumers-gdpr-brand-experience/
22. https://www.ama.org/2020/11/11/avoid-becoming-the-target-of-penalizing-privacy-laws/

Reducing risk and creating stronger ties

Privacy and marketing are constantly colliding. This means without the proper training or data privacy knowledge, businesses can overlook privacy and compliance at the end of a campaign instead of the beginning, always leaving the details up to the legal department or compliance team. Detailed privacy functions such as consent, cookie limitations, data subject rights, data mapping and minimization may be well known by an analytics department, but not necessarily by all marketing professionals individually. Because compliance is an ongoing process that reaches into many aspects of a marketing program, building a strong commitment to user privacy could mean offering more specialized training throughout marketing departments.

KEY TAKEAWAY

Having a deeper understanding of the risks and benefits to these regulations can reduce risk of exposure to non-compliance issues and help to reinforce and bolster dedication to keeping user data safe.

Leveraging consumer privacy as a competitive advantage

With an opportunistic outlook, businesses should partner with marketing firms that mindfully leverage their data, without the risk of non-compliance, positioning them for success in the new era. As privacy grows increasingly important to consumers, agency partners that cater to this need can help their clients gain a competitive advantage over those that do not.
At Levelwing, we understand the challenges ahead, and look forward to exercising our skills in deeper analysis as changes to data privacy regulations evolve. We strive for the highest standards together with our clients and vendors, keeping data safe and in accordance with the regulations it is subject to. We implement cross team training to ensure compliance across all departments, as well as managing platform audits on a consistent basis. Our team endeavors to be intentional when determining what information is collected, who it is collected from, why it is collected, and how it is used.

LEVELWING

**Disclaimer: This does not and is not intended to offer any legal advice. All information and content is for general information purposes only.

IF YOU WOULD LIKE TO SPEAK WITH SOMEONE AT LEVELWING ABOUT THE FUTURE OF DATA PRIVACY PLEASE CONTACT:

Steve Parker Jr.
CEO & Co-Founder
sparker@levelwing.com
843-631-4587